Theoretical Computer Science 106 (1992) 221–241
Elsevier

Complexity of logical theories involving coprimality

Pascal Michel

Université Paris 7, 59 rue du Cardinal Lemoine, 75005 Paris, France

Communicated by D. Perrin
Received December 1990
Revised April 1991

Abstract

Michel, P., Complexity of logical theories involving coprimality, Theoretical Computer Science 106 (1992) 221–241.

Upper bounds on the computational complexity of some logical theories are proved. The theory $\mathrm{Th}(\mathcal{P}_f(\mathbb{N}), \subseteq)$ of finite subsets of $\mathbb{N}$ is proved to be in $\bigcup_{c>0}\mathrm{ATIME\text{-}ALT}(2^{cn}, n)$. The same result is proved for the theories $\mathrm{Th}(\mathbb{N}, \perp)$, $\mathrm{Th}(\mathbb{N}, \perp, \times)$ and $\mathrm{Th}(\mathbb{N}, \perp, \times, 2x, x^2, 2^x)$, where $\perp$ denotes coprimality of numbers. The theory $\mathrm{Th}(\mathbb{N}, =, \perp)$ is proved to be in $\bigcup_{c>0}\mathrm{ATIME\text{-}ALT}(2^{cn^2}, n)$.

1. Introduction

It is well known that *complete number theory*, i.e. the theory of the structure $\langle \mathbb{N}, =, +, \times \rangle$, is undecidable. When we drop one of the operations $+$ or $\times$, the theories $\mathrm{Th}(\mathbb{N}, =, +)$ and $\mathrm{Th}(\mathbb{N}, =, \times)$ we obtain are decidable [19, 16, 25]. The computational complexity of these theories has been studied [3, 4, 8–11, 17, 18, 20, 21], eventually showing that $\mathrm{Th}(\mathbb{N}, =, +)$ is complete for $\bigcup_{c>0}\mathrm{ATIME\text{-}ALT}(2^{2^{cn}}, n)$, and $\mathrm{Th}(\mathbb{N}, =, \times)$ is complete for $\bigcup_{c>0}\mathrm{ATIME\text{-}ALT}(2^{2^{2^{cn}}}, n)$ [8].

Many relations and functions can be defined in $\langle \mathbb{N}, =, +, \times \rangle$. First, consider the following weakenings of $+$: the linear ordering $\leqslant$, which is definable in $\langle \mathbb{N}, =, + \rangle$, and the successor function S, which is definable in $\langle \mathbb{N}, \leqslant \rangle$. Next consider the following weakenings of $\times$: the partial ordering $|$ of divisibility, which is definable in $\langle \mathbb{N}, =, \times \rangle$, and the binary relation $\perp$ of coprimality, which is definable in $\langle \mathbb{N}, | \rangle$. Note that $=$ is definable in $\langle \mathbb{N}, \leqslant \rangle$ and $\langle \mathbb{N}, | \rangle$.

What happens to the theory $\mathrm{Th}(\mathbb{N}, =, \leqslant, |, \perp, S, +, \times)$ if we drop some of these relations or functions? Robinson [23] has proved that in $\langle \mathbb{N}, S, | \rangle$ we can define all relations and functions of complete number theory. Woods [27] has proved the same

result for $\langle \mathbb{N}, \leqslant, \perp \rangle$ and $\langle \mathbb{N}, \perp, + \rangle$. It is still open whether the same result holds for the structures $\langle \mathbb{N}, S, \perp \rangle$ and $\langle \mathbb{N}, =, S, \perp \rangle$, but Woods [27] has proved that their theories are undecidable. This shows that if a weakening of $+$ and one of $\times$ are put together in a structure, then we get an undecidable theory.

It follows from these undecidability results that among the theories obtained from $\mathrm{Th}(\mathbb{N}, =, \leqslant, |, \perp, S, +, \times)$ by dropping symbols of relations or functions, the maximal decidable ones are exactly $\mathrm{Th}(\mathbb{N}, =, \leqslant, S, +)$ (i.e. $\mathrm{Th}(\mathbb{N}, =, +)$), and $\mathrm{Th}(\mathbb{N}, =, |, \perp, \times)$ (i.e. $\mathrm{Th}(\mathbb{N}, =, \times)$). What happens if we drop some symbols from the last two theories? It is known that $\mathrm{Th}(\mathbb{N}, =)$, $\mathrm{Th}(\mathbb{N}, =, S)$ and $\mathrm{Th}(\mathbb{N}, \leqslant)$ are PSPACE-complete [10]. The study of $\mathrm{Th}(\mathbb{N}-\{0\}, |)$ by Volger [26], improving Michel [15], showed that this theory is in $\bigcup_{c>0} \mathrm{ATIME\text{-}ALT}(2^{cn^2 \log n}, n)$ and is complete in $\bigcup_{k>0} \mathrm{ATIME\text{-}ALT}(2^{cn^k}, n)$ for the polynomial-time many-one reducibility.

We shall consider in this paper the complexity of the theories of the following structures, the last ones left unsettled: $\langle \mathbb{N}, \perp \rangle$, $\langle \mathbb{N}, \perp, \times \rangle$ and $\langle \mathbb{N}, =, \perp \rangle$. We shall prove in Section 4 that $\mathrm{Th}(\mathbb{N}, \perp)$ and $\mathrm{Th}(\mathbb{N}, \perp, \times)$ are in $\bigcup_{c>0} \mathrm{ATIME\text{-}ALT}(2^{cn}, n)$, and that $\mathrm{Th}(\mathbb{N}, =, \perp)$ is in $\bigcup_{c>0} \mathrm{ATIME\text{-}ALT}(2^{cn^2}, n)$. These upper bounds almost match the following lower bound (Theorem 4.2): there is a $c>0$ such that none of these theories are in $\mathrm{ATIME\text{-}ALT}(2^{cn/\log n}, cn)$.

In fact, we shall see in Section 4 that $\mathrm{Th}(\mathbb{N}, \perp)$ has essentially the same complexity as the theory $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), \subseteq)$ of the lattice of finite subsets of $\mathbb{N}$. This theory was studied by Volger [26], who proved that

$$\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), \subseteq) \in \bigcup_{c>0} \mathrm{ATIME\text{-}ALT}(2^{cn^2}, n),$$

using a general theorem of Ferrante and Rackoff [10] on the complexity of the theory of the countable weak direct power of a structure. A more direct approach, which does not use this general theorem, allows us to improve this result. We prove in Section 3 that

$$\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), \subseteq) \in \bigcup_{c>0} \mathrm{ATIME\text{-}ALT}(2^{cn}, n).$$

We also consider upper and lower bounds on the complexity of various related theories, such as

$$\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), =, \subseteq, \cap, \cup, \perp, \emptyset) \quad \text{and} \quad \mathrm{Th}(\mathscr{P}_f(\mathbb{N}) \cup \{\mathbb{N}\}, \subseteq).$$

Finally, in Section 5, we study the effect of adding the functions $2x, x^2, 2^x$ to the structures $\langle \mathbb{N}, = \rangle$ and $\langle \mathbb{N}, \perp, \times \rangle$. We prove that $\mathrm{Th}(\mathbb{N}, =, 2x)$, $\mathrm{Th}(\mathbb{N}, =, x^2)$ and $\mathrm{Th}(\mathbb{N}, =, 2^x)$ are PSPACE-complete, and

$$\mathrm{Th}(\mathbb{N}, \perp, \times, 2x, x^2, 2^x) \in \bigcup_{c>0} \mathrm{ATIME\text{-}ALT}(2^{cn}, n).$$

2. Preliminaries

We refer to [7, 10] for detailed logical preliminaries. Let $\mathscr{A} = \langle A, R_1, \dots, R_l \rangle$ be a *structure*. A is the nonempty *domain* of $\mathscr{A}$, $R_i \subseteq A^{\gamma_i}$ are relations on A for $1 \leqslant i \leqslant l$. $\{R_1, \dots, R_l\}$ is the *vocabulary* of the structure. We shall also consider structures with functions and constants; whenever it will be the case, we shall see that their analysis can be reduced to the analysis of structures with relations only. We denote by $\bar{a}_k$ a k-tuple $(a_1, \dots, a_k) \in A^k$.

Let φ be a formula involving the logical symbols $\neg$, $\wedge$, $\vee$, $\forall$, $\exists$, the parentheses (, and), formal variables $v_0, v_1, v_{10}, \dots$ with subscripts written in binary, and relation symbols that are for simplicity denoted as are the relations of $\mathscr{A}$: $R_1, \dots, R_l$. If $\bar{x}_k = (x_1, \dots, x_k)$ are the free variables of $\varphi = \varphi(\bar{x}_k)$, and $\bar{a}_k \in A^k$, we write $\mathscr{A} \models \varphi(\bar{a}_k)$ if $\varphi(\bar{a}_k)$ is true in $\mathscr{A}$. We also say in that case that $\bar{a}_k$ satisfies $\varphi(\bar{x}_k)$.

A *sentence* is a formula with no free variables. A sentence is in *prenex normal form* if it is of the form $Q_1 x_1 \dots Q_k x_k \varphi(\bar{x}_k)$, where $Q_1, \dots, Q_k$ are quantifiers, and $\varphi(\bar{x}_k)$ is quantifier-free. A sentence can be put in prenex normal form in deterministic polynomial time. This procedure makes the length longer in the stage of renaming variables, but (this is the crucial point) does not increase the number of quantifiers.

The *theory* of a structure $\mathscr{A}$ is the set of sentences which are true in $\mathscr{A}$: $\mathrm{Th}(\mathscr{A}) = \{\varphi : \mathscr{A} \models \varphi\}$. We write $\mathrm{Th}(A, R_1, \dots, R_l)$ for $\mathrm{Th}(\langle A, R_1, \dots, R_l \rangle)$. The theory is *decidable* if this set is recursive.

The following theorem is implicit in [10, pp. 30–31 and 34–35]; see also [14, pp. 209–210]. It involves a structure $\mathscr{A} = \langle A, R_1, \dots, R_l \rangle$, a family E_k^n of equivalence relations on A^k, a norm, that is a function $\|\cdot\|$ from A into $\mathbb{N}$, and a function $H : \mathbb{N}^3 \to \mathbb{N}$. If $x \in A$ and $m \in \mathbb{N}$, we write $x \preceq m$ whenever $\|x\| \leqslant m$.

Theorem 2.1. *Let $\mathscr{A} = \langle A, \dots \rangle$ be a structure, together with equivalence relations E_k^n on A^k, a norm $\|\cdot\|$, a function $H(n, k, m)$, and $\mu \in \mathbb{N}$, satisfying the following conditions:*

(i) *For any $k \in \mathbb{N} - \{0\}$, any $m \geqslant \mu$, any $\bar{a}_k, \bar{b}_k \in A^k$, if $\bar{a}_k E_k^{n+1} \bar{b}_k$ and $\forall i\ 1 \leqslant i \leqslant k \Rightarrow \|b_i\| \leqslant m$, then for all $a_{k+1} \in A$ there exists a $b_{k+1} \in A$ such that $\bar{a}_{k+1} E_{k+1}^n \bar{b}_{k+1}$ and $\|b_{k+1}\| \leqslant H(n, k, m)$.*

(ii) *For any $k \in \mathbb{N} - \{0\}$, for any $\bar{a}_k, \bar{b}_k \in A^k$, if $\bar{a}_k E_k^0 \bar{b}_k$, then $\bar{a}_k$ and $\bar{b}_k$ satisfy the same atomic formulas.*

Let $k \in \mathbb{N}$. Let $Q_1 x_1 \dots Q_k x_k F(\bar{x}_k)$ be a sentence in prenex normal form (F quantifier-free). Let $\langle m_i : 0 \leqslant i \leqslant k \rangle \in \mathbb{N}^{k+1}$ satisfying $\mu \leqslant m_0 \leqslant m_1 \leqslant \cdots \leqslant m_k$, and $\forall i\ 1 \leqslant i \leqslant k \Rightarrow m_i \geqslant H(k-i, i-1, m_{i-1})$.

Then $\mathscr{A} \models Q_1 x_1 \dots Q_k x_k F(\bar{x}_k)$ if and only if $\mathscr{A} \models Q_1 x_1 \preceq m_1 \dots Q_k x_k \preceq m_k F(\bar{x}_k)$.

We refer to [12, 1] for detailed preliminaries on computational complexity. We use the complexity measure ATIME-ALT. *Alternating Turing machines* (ATM) are a generalization of nondeterministic Turing machines. A state of an ATM is either final (accepting or rejecting) or *existential* or *universal*. An existential configuration (consisting of state, tape contents and head positions) leads to acceptance if some one of its

immediate successors leads to acceptance. A universal configuration leads to acceptance if all its immediate successors lead to acceptance. More formally, an *accepting computation subtree* of an ATM M on an input x is a finite subtree of the tree of all configurations of M on x verifying the following conditions: the root is the initial configuration of M on x, existential configurations have only one child, universal configurations have all their immediate successors as children, and all leaves are accepting.

An ATM M is time-bounded by $T(n)$ and $A(n)$-alternation bounded if for any accepted input x, there is an accepting computation subtree of M on x of height at most $T(|x|)$, and such that on any branch from the root to an accepting leaf there are at most $A(|x|)-1$ alternations of universal and existential configurations. ATIME-ALT($T(n), A(n)$) is the class of languages accepted by ATMs which are time-bounded by $T(n)$ and $A(n)$-alternation bounded. See [2, 6] for more details on ATMs.

ATIME-ALT is a complexity measure especially well suited to the analysis of decidable theories. In fact, alternations of existential and universal states are used to simulate alternations of existential and universal quantifiers of the input sentence. To perform this simulation, it is necessary that the quantified variables should be bounded. This is what is secured by the conclusions of Theorem 2.1, once its hypotheses are verified. See [3, 4, 8, 13] for examples of discussions and uses of the ATIME-ALT measure.

We shall use two reductions: the standard polynomial-time many–one reduction $\leqslant_m^p$, and the reset log–lin reduction $\leqslant_m^{rll}$ introduced by Compton and Henson [8]. For any sets A and $B \subseteq \Sigma^*$, $A \leqslant_m^{rll} B$ if there is a mapping $f: \Sigma^* \to \Sigma^*$, such that $\forall x \in \Sigma^*$ $x \in A \Leftrightarrow f(x) \in B$ and f is computable by a log-space, linear-time bounded Turing machine which has the capability to reset the input tape head to the initial input cell on k moves during a computation, where k is fixed for all inputs; on all other moves the input tape head remains in place or moves one cell to the right.

Our notations are standard. $\mathscr{P}_f(\mathbb{N})$ denotes the set of finite subsets of $\mathbb{N}$ and $\mathscr{P}_\infty(\mathbb{N})$ the set of infinite subsets of $\mathbb{N}$. The symbols $+$ and $\times$ denote the binary functions (and not the graphs of these functions). The same symbol $\perp$ will denote both disjointness of subsets of $\mathbb{N}$ and coprimality of natural numbers, but its meaning will always be clear from the context. For $i \geqslant 1$, p_i is the ith prime number. We denote by $|\varphi|$ the length of formula φ, i.e. the number of letters of φ. Recall that the alphabet on which φ is written is finite, and that the subscripts of variables are written in binary. All logarithms are in base two.

3. Complexity of the theory of finite subsets of $\mathbb{N}$

In this section, we give an upper bound for $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), \subseteq)$, where $\mathscr{P}_f(\mathbb{N})$ is the set of finite subsets of $\mathbb{N}$. Afterwards, we consider lower bounds for this theory, and we study related theories which have the same complexity.

Volger [26] considers $\langle \mathscr{P}_f(\mathbb{N}), \subseteq \rangle$ as the countable weak direct power of $\langle \{0,1\}, \leqslant \rangle$. Ferrante and Rackoff [10] (see also [21]) give a general method to obtain the complexity of the weak direct power of a structure from the complexity of this structure. Volger uses this method to prove that

$$\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), \subseteq) \in \bigcup_{c>0} \mathrm{ATIME\text{-}ALT}(2^{cn^2}, n).$$

We shall here improve that result by the direct application of Theorem 2.1. We verify in the first two lemmas below that the hypotheses of this theorem are satisfied.

Definitions 3.1.

(i) For any $A \in \mathscr{P}_f(\mathbb{N})$, let $1A = A$ and $-1A = -A = \mathbb{N} - A$.

(ii) For any $\bar{A}_k = (A_1, \ldots, A_k) \in \mathscr{P}_f(\mathbb{N})^k$, and any $\bar{\varepsilon}_k = (\varepsilon_1, \ldots, \varepsilon_k) \in \{-1, 1\}^k$, let $\bar{\varepsilon}_k \bar{A}_k = \varepsilon_1 A_1 \cap \cdots \cap \varepsilon_k A_k$.

(iii) Let $\bar{\varepsilon}_k^{\infty} = (-1, \ldots, -1) \in \{-1, 1\}^k$.

These definitions allow an easy way to deal with the 2^k (possibly empty) subsets of $\mathbb{N}$ that constitute the partition defined by the intersections between k subsets and their complements.

The following proposition states without proof some straightforward properties of these subsets.

Proposition 3.2.

(i) $\forall \bar{A}_k \in \mathscr{P}_f(\mathbb{N})^k \; \forall \bar{\varepsilon}_k \in \{-1, 1\}^k \; \bar{\varepsilon}_k \neq \bar{\varepsilon}_k^{\infty} \Rightarrow \bar{\varepsilon}_k \bar{A}_k \in \mathscr{P}_f(\mathbb{N})$.

(ii) $\forall \bar{A}_k \in \mathscr{P}_f(\mathbb{N})^k \; \bar{\varepsilon}_k^{\infty} \bar{A}_k$ *is infinite.*

(iii) $\forall \bar{A}_k \in \mathscr{P}_f(\mathbb{N})^k \; \forall \bar{\varepsilon}_k, \bar{\varepsilon}_k' \in \{-1, 1\}^k \; \bar{\varepsilon}_k \neq \bar{\varepsilon}_k' \Rightarrow \bar{\varepsilon}_k \bar{A}_k \cap \bar{\varepsilon}_k' \bar{A}_k = \emptyset$.

(iv) $\forall A_k \in \mathscr{P}_f(\mathbb{N})^k \bigcup \{\bar{\varepsilon}_k \bar{A}_k : \bar{\varepsilon}_k \in \{-1, 1\}^k\} = \mathbb{N}$.

(v) *Let* $\langle P_1, \ldots, P_{2^k} \rangle$ *be an ordered partition of* $\mathbb{N}$, *satisfying* $\forall i \; 1 \leqslant i \leqslant 2^k - 1 \Rightarrow P_i \in \mathscr{P}_f(\mathbb{N})$ *and* $P_{2^k} \in \mathscr{P}_{\infty}(\mathbb{N})$. *Then there is a unique* $\bar{A}_k \in \mathscr{P}_f(\mathbb{N})^k$ *such that* $\langle P_1, \ldots, P_{2^k} \rangle = \langle \bar{\varepsilon}_k \bar{A}_k : \bar{\varepsilon}_k \in \{-1, 1\}^k \rangle$, *where* $\{-1, 1\}^k$ *is ordered according to the inverse lexicographic order*: $(1, \ldots, 1) < \cdots < (-1, \ldots, -1)$.

(vi) $\forall \bar{A}_k \in \mathscr{P}_f(\mathbb{N})^k \forall C \in \mathscr{P}_f(\mathbb{N}) \forall j 1 \leqslant j \leqslant k \Rightarrow [C \cap A_j = \emptyset \Leftrightarrow \forall \bar{\varepsilon}_k \in \{-1, 1\}^k \quad (\varepsilon_j = 1 \Rightarrow C \cap \bar{\varepsilon}_k \bar{A}_k = \emptyset)]$.

We now define the family of equivalence relations E_k^n.

Definitions 3.3. (i) Let $n, p, q \in \mathbb{N}$. $p \underset{n}{\simeq} q$ if either $p = q < 2^n$ or $p \geqslant 2^n$ and $q \geqslant 2^n$.

(ii) Let $n, k \in \mathbb{N}, k \geqslant 1$. Let $\bar{A}_k, \bar{B}_k \in \mathscr{P}_f(\mathbb{N})^k$. $\bar{A}_k E_k^n \bar{B}_k$ if $\forall \bar{\varepsilon}_k \in \{-1, 1\}^k$ $\mathrm{card}(\bar{\varepsilon}_k \bar{A}_k) \underset{n}{\simeq} \mathrm{card}(\bar{\varepsilon}_k \bar{B}_k)$.

(iii) If $A \in \mathscr{P}_f(\mathbb{N})$, $\max(A)$ is the greatest member of A. By convention $\max(\emptyset) = 0$.

We can now verify that the hypotheses of Theorem 2.1 are satisfied.

Lemma 3.4. *Let* $\bar{A}_k, \bar{B}_k \in \mathscr{P}_f(\mathbb{N})^k$ *such that* $\bar{A}_k E_k^{n+1} \bar{B}_k$. *Then for any* $A_{k+1} \in \mathscr{P}_f(\mathbb{N})$, *there is a* $B_{k+1} \in \mathscr{P}_f(\mathbb{N})$ *such that* $\bar{A}_{k+1} E_{k+1}^n \bar{B}_{k+1}$.

If, moreover, $\forall j\, 1 \leqslant j \leqslant k \Rightarrow \max(B_j) \leqslant m$, *then we can choose* B_{k+1} *such that* $\max(B_{k+1}) \leqslant m + 2^n$.

Proof. At first, we describe the construction of B_{k+1}. Let $\bar{A}_k, \bar{B}_k \in \mathscr{P}_f(\mathbb{N})^k$ such that $\bar{A}_k, E_k^{n+1} \bar{B}_k$. Let $A_{k+1} \in \mathscr{P}_f(\mathbb{N})$. We have, for any $\bar{\varepsilon}_k \in \{-1, 1\}^k$, $\mathrm{card}(\bar{\varepsilon}_k \bar{A}_k) \underset{n+1}{\simeq} \mathrm{card}(\bar{\varepsilon}_k \bar{B}_k)$, i.e. either $\mathrm{card}(\bar{\varepsilon}_k \bar{A}_k) = \mathrm{card}(\bar{\varepsilon}_k \bar{B}_k) < 2^{n+1}$, or $\mathrm{card}(\bar{\varepsilon}_k \bar{A}_k)$ and $\mathrm{card}(\bar{\varepsilon}_k \bar{B}_k) \geqslant 2^{n+1}$. By Proposition 3.2(v), B_{k+1} is completely determined by $\langle \bar{\varepsilon}_{k+1} \bar{B}_{k+1} : \bar{\varepsilon}_{k+1} \in \{-1, 1\}^{k+1} \rangle$.

Let $\bar{\varepsilon}_k \in \{-1, 1\}^k$.

- if $\mathrm{card}(A_{k+1} \cap \bar{\varepsilon}_k \bar{A}_k) < \mathrm{card}(-A_{k+1} \cap \bar{\varepsilon}_k \bar{A}_k)$ (notably if $\bar{\varepsilon}_k = \bar{\varepsilon}_k^{\infty}$), then we put in $B_{k+1} \cap \bar{\varepsilon}_k \bar{B}_k$ the $\min(2^n, \mathrm{card}(A_{k+1} \cap \bar{\varepsilon}_k \bar{A}_k))$ smallest members of $\bar{\varepsilon}_k \bar{B}_k$ (the other members of $\bar{\varepsilon}_k \bar{B}_k$ are put in $-B_{k+1} \cap \bar{\varepsilon}_k \bar{B}_k$).
- if $\mathrm{card}(A_{k+1} \cap \bar{\varepsilon}_k \bar{A}_k) \geqslant \mathrm{card}(-A_{k+1} \cap \bar{\varepsilon}_k \bar{A}_k)$ (hence, $\bar{\varepsilon}_k \neq \bar{\varepsilon}_k^{\infty}$), then we put in $-B_{k+1} \cap \bar{\varepsilon}_k \bar{B}_k$ the $\min(2^n, \mathrm{card}(-A_{k+1} \cap \bar{\varepsilon}_k \bar{A}_k))$ greatest members of $\bar{\varepsilon}_k \bar{B}_k$, i.e. we put in $B_{k+1} \cap \bar{\varepsilon}_k \bar{B}_k$ the $\mathrm{card}(\bar{\varepsilon}_k \bar{B}_k) - \min(2^n, \mathrm{card}(-A_{k+1} \cap \bar{\varepsilon}_k \bar{A}_k))$ smallest members of $\bar{\varepsilon}_k \bar{B}_k$.

Now we prove that for any $\bar{\varepsilon}_{k+1} \in \{-1, 1\}^{k+1}$, we have $\mathrm{card}(\bar{\varepsilon}_{k+1} \bar{A}_{k+1}) \underset{n}{\simeq} \mathrm{card}(\bar{\varepsilon}_{k+1} \bar{B}_{k+1})$. We have to consider many cases, which is tedious, but the arguments in each case are rather straightforward.

Case 1: $\mathrm{card}(\bar{\varepsilon}_k \bar{A}_k) = \mathrm{card}(\bar{\varepsilon}_k \bar{B}_k) < 2^{n+1}$ and $\mathrm{card}(A_{k+1} \cap \bar{\varepsilon}_k \bar{A}_k) < \mathrm{card}(-A_{k+1} \cap \bar{\varepsilon}_k \bar{A}_k)$.

Then $\mathrm{card}(A_{k+1} \cap \bar{\varepsilon}_k \bar{A}_k) + \mathrm{card}(-A_{k+1} \cap \bar{\varepsilon}_k \bar{A}_k) = \mathrm{card}(\bar{\varepsilon}_k \bar{A}_k) < 2^{n+1}$; thus, $\mathrm{card}(A_{k+1} \cap \bar{\varepsilon}_k \bar{A}_k) < 2^n$. Therefore,

$$\begin{aligned} \mathrm{card}(B_{k+1} \cap \bar{\varepsilon}_k \bar{B}_k) &= \min(2^n, \mathrm{card}(A_{k+1} \cap \bar{\varepsilon}_k \bar{A}_k)) \\ &= \mathrm{card}(A_{k+1} \cap \bar{\varepsilon}_k \bar{A}_k) \end{aligned}$$

and

$$\begin{aligned} \mathrm{card}(-B_{k+1} \cap \bar{\varepsilon}_k \bar{B}_k) &= \mathrm{card}(\bar{\varepsilon}_k \bar{B}_k) - \mathrm{card}(B_{k+1} \cap \bar{\varepsilon}_k \bar{B}_k) \\ &= \mathrm{card}(\bar{\varepsilon}_k \bar{A}_k) - \mathrm{card}(A_{k+1} \cap \bar{\varepsilon}_k \bar{A}_k) \\ &= \mathrm{card}(-A_{k+1} \cap \bar{\varepsilon}_k \bar{A}_k). \end{aligned}$$

Case 2: $\mathrm{card}(\bar{\varepsilon}_k \bar{A}_k) = \mathrm{card}(\bar{\varepsilon}_k \bar{B}_k) < 2^{n+1}$ and $\mathrm{card}(A_{k+1} \cap \bar{\varepsilon}_k \bar{A}_k) \geqslant \mathrm{card}(-A_{k+1} \cap \bar{\varepsilon}_k \bar{A}_k)$.

Then $\mathrm{card}(-A_{k+1} \cap \bar{\varepsilon}_k \bar{A}_k) < 2^n$. Therefore,

$$\begin{aligned} \mathrm{card}(-B_{k+1} \cap \bar{\varepsilon}_k \bar{B}_k) &= \min(2^n, \mathrm{card}(-A_{k+1} \cap \bar{\varepsilon}_k \bar{A}_k) \\ &= \mathrm{card}(-A_{k+1} \cap \bar{\varepsilon}_k \bar{A}_k), \end{aligned}$$

and

$$\begin{aligned}\operatorname{card}(B_{k+1}\cap\bar{\varepsilon}_k\bar{B}_k)&=\operatorname{card}(\bar{\varepsilon}_k\bar{B}_k)-\operatorname{card}(-B_{k+1}\cap\bar{\varepsilon}_k\bar{B}_k)\\&=\operatorname{card}(\bar{\varepsilon}_k\bar{A}_k)-\operatorname{card}(-A_{k+1}\cap\bar{\varepsilon}_k\bar{A}_k)\\&=\operatorname{card}(A_{k+1}\cap\bar{\varepsilon}_k\bar{A}_k).\end{aligned}$$

Case 3: $\operatorname{card}(\bar{\varepsilon}_k\bar{A}_k)$ and $\operatorname{card}(\bar{\varepsilon}_k\bar{B}_k)\geqslant 2^{n+1}$, $\operatorname{card}(A_{k+1}\cap\bar{\varepsilon}_k\bar{A}_k)<\operatorname{card}(-A_{k+1}\cap\bar{\varepsilon}_k\bar{A}_k)$ and $\operatorname{card}(A_{k+1}\cap\bar{\varepsilon}_k\bar{A}_k)<2^n$.

Then

$$\operatorname{card}(B_{k+1}\cap\bar{\varepsilon}_k\bar{B}_k)=\min(2^n,\operatorname{card}(A_{k+1}\cap\bar{\varepsilon}_k\bar{A}_k))=\operatorname{card}(A_{k+1}\cap\bar{\varepsilon}_k\bar{A}_k)$$

and

$$\operatorname{card}(-B_{k+1}\cap\bar{\varepsilon}_k\bar{B}_k)+\operatorname{card}(B_{k+1}\cap\bar{\varepsilon}_k\bar{B}_k)=\operatorname{card}(\bar{\varepsilon}_k\bar{B}_k)\geqslant 2^{n+1};$$

thus, $\operatorname{card}(-B_{k+1}\cap\bar{\varepsilon}_k\bar{B}_k)\geqslant 2^n$.

Likewise,

$$\operatorname{card}(-A_{k+1}\cap\bar{\varepsilon}_k\bar{A}_k)+\operatorname{card}(A_{k+1}\cap\bar{\varepsilon}_k\bar{A}_k)=\operatorname{card}(\bar{\varepsilon}_k\bar{A}_k)\geqslant 2^{n+1};$$

thus, $\operatorname{card}(-A_{k+1}\cap\bar{\varepsilon}_k\bar{A}_k)\geqslant 2^n$.

Case 4: $\operatorname{card}(\bar{\varepsilon}_k\bar{A}_k)$ and $\operatorname{card}(\bar{\varepsilon}_k\bar{B}_k)\geqslant 2^{n+1}$, $\operatorname{card}(A_{k+1}\cap\bar{\varepsilon}_k\bar{A}_k)<\operatorname{card}(-A_{k+1}\cap\bar{\varepsilon}_k\bar{A}_k)$, and $\operatorname{card}(A_{k+1}\cap\bar{\varepsilon}_k\bar{A}_k)\geqslant 2^n$.

Then $\operatorname{card}(B_{k+1}\cap\bar{\varepsilon}_k\bar{B}_k)=\min(2^n,\operatorname{card}(A_{k+1}\cap\bar{\varepsilon}_k\bar{A}_k))=2^n$; thus, $\operatorname{card}(A_{k+1}\cap\bar{\varepsilon}_k\bar{A}_k)$ and $\operatorname{card}(B_{k+1}\cap\bar{\varepsilon}_k\bar{B}_k)\geqslant 2^n$.

On the other hand,

$$\begin{aligned}\operatorname{card}(-B_{k+1}\cap\bar{\varepsilon}_k\bar{B}_k)&=\operatorname{card}(\bar{\varepsilon}_k\bar{B}_k)-\operatorname{card}(B_{k+1}\cap\bar{\varepsilon}_k\bar{B}_k)\\&=\operatorname{card}(\bar{\varepsilon}_k\bar{B}_k)-2^n\geqslant 2^{n+1}-2^n=2^n,\end{aligned}$$

and

$$\operatorname{card}(-A_{k+1}\cap\bar{\varepsilon}_k\bar{A}_k)>\operatorname{card}(A_{k+1}\cap\bar{\varepsilon}_k\bar{A}_k)\geqslant 2^n.$$

Case 5: $\operatorname{card}(\bar{\varepsilon}_k\bar{A}_k)$ and $\operatorname{card}(\bar{\varepsilon}_k\bar{B}_k)\geqslant 2^{n+1}$, and $\operatorname{card}(A_{k+1}\cap\bar{\varepsilon}_k\bar{A}_k)\geqslant\operatorname{card}(-A_{k+1}\cap\bar{\varepsilon}_k\bar{A}_k)$.

Then $\operatorname{card}(-B_{k+1}\cap\bar{\varepsilon}_k\bar{B}_k)=\min(2^n,\operatorname{card}(-A_{k+1}\cap\bar{\varepsilon}_k\bar{A}_k))$; thus, if $\operatorname{card}(-A_{k+1}\cap\bar{\varepsilon}_k\bar{A}_k)<2^n$, then $\operatorname{card}(-B_{k+1}\cap\bar{\varepsilon}_k\bar{B}_k)=\operatorname{card}(-A_{k+1}\cap\bar{\varepsilon}_k\bar{A}_k)$, and if $\operatorname{card}(-A_{k+1}\cap\bar{\varepsilon}_k\bar{A}_k)\geqslant 2^n$, then $\operatorname{card}(-B_{k+1}\cap\bar{\varepsilon}_k\bar{B}_k)=2^n$, and $\operatorname{card}(-A_{k+1}\cap\bar{\varepsilon}_k\bar{A}_k)$ and $\operatorname{card}(-B_{k+1}\cap\bar{\varepsilon}_k\bar{B}_k)\geqslant 2^n$.

On the other hand,

$$\begin{aligned}\operatorname{card}(B_{k+1}\cap\bar{\varepsilon}_k\bar{B}_k)&=\operatorname{card}(\bar{\varepsilon}_k\bar{B}_k)-\operatorname{card}(-B_{k+1}\cap\bar{\varepsilon}_k\bar{B}_k)\\&\geqslant 2^{n+1}-2^n=2^n,\end{aligned}$$

and

$$\begin{aligned}\operatorname{card}(A_{k+1} \cap \bar{\varepsilon}_k \bar{A}_k) &\geqslant \tfrac{1}{2}(\operatorname{card}(A_{k+1} \cap \bar{\varepsilon}_k \bar{A}_k) + \operatorname{card}(-A_{k+1} \cap \bar{\varepsilon}_k \bar{A}_k)) \\ &= \tfrac{1}{2}\operatorname{card}(\bar{\varepsilon}_k \bar{A}_k) \geqslant 2^n.\end{aligned}$$

This proves that $\bar{A}_{k+1} E^n_{k+1} \bar{B}_{k+1}$. Now we complete the proof of the lemma by showing that if $\forall j\, 1 \leqslant j \leqslant k \Rightarrow \max(B_j) \leqslant m$, then $\max(B_{k+1}) \leqslant m + 2^n$.

The members of B_{k+1} which are in $\bigcup_{j=1}^{k} B_j$ are obviously bounded by m. The members of B_{k+1} which are outside $\bigcup_{j=1}^{k} B_j$ are those from $B_{k+1} \cap \bar{\varepsilon}_k^{\times} \bar{B}_k$. They are in number at most $\min(2^n, \operatorname{card}(A_{k+1} \cap \bar{\varepsilon}_k^{\times} \bar{A}_k)) \leqslant 2^n$, and they are the smallest ones. At worst, they are the following numbers: $\max(\bigcup_j B_j)+1$, $\max(\bigcup_j B_j)+2, \ldots,$ $\max(\bigcup_j B_j)+2^n$. Therefore, $\max(B_{k+1}) \leqslant m + 2^n$. □

Lemma 3.5. *Let $k \in \mathbb{N} - \{0\}$ and $\bar{A}_k, \bar{B}_k \in \mathscr{P}_f(\mathbb{N})^k$. If $\bar{A}_k E^0_k \bar{B}_k$, then $\bar{A}_k$ and $\bar{B}_k$ satisfy the same atomic formulas (in the vocabulary of inclusion).*

Proof. By definition, if $\bar{A}_k E^0_k \bar{B}_k$, then for any $\bar{\varepsilon}_k \in \{-1, 1\}^k$, $\operatorname{card}(\bar{\varepsilon}_k \bar{A}_k) \underset{0}{\simeq} \operatorname{card}(\bar{\varepsilon}_k \bar{B}_k)$, i.e. either $\bar{\varepsilon}_k \bar{A}_k = \bar{\varepsilon}_k \bar{B}_k = \emptyset$, or $\bar{\varepsilon}_k \bar{A}_k \neq \emptyset$ and $\bar{\varepsilon}_k \bar{B}_k \neq \emptyset$. Therefore, $\forall \bar{\varepsilon}_k \in \{-1, 1\}^k$ $\bar{\varepsilon}_k \bar{A}_k = \emptyset \Leftrightarrow \bar{\varepsilon}_k \bar{B}_k = \emptyset$. Thus, for any i, j, $1 \leqslant i, j \leqslant k$, we have

$$\begin{aligned}A_i \subseteq A_j &\Leftrightarrow \forall \bar{\varepsilon}_k \in \{-1, 1\}^k \ (\varepsilon_i = 1 \text{ and } \varepsilon_j = -1) \Rightarrow \bar{\varepsilon}_k \bar{A}_k = \emptyset \\ &\Leftrightarrow \forall \bar{\varepsilon}_k \in \{-1, 1\}^k \ (\varepsilon_i = 1 \text{ and } \varepsilon_j = -1) \Rightarrow \bar{\varepsilon}_k \bar{B}_k = \emptyset \\ &\Leftrightarrow B_i \subseteq B_j. \quad \square\end{aligned}$$

Lemma 3.6. *Let $k \in \mathbb{N} - \{0\}$ and $Q_1 X_1 \ldots Q_k X_k F(\bar{X}_k)$ be a sentence, with $F(\bar{X}_k)$ quantifier-free. Then $\langle \mathscr{P}_f(\mathbb{N}), \subseteq \rangle \models Q_1 X_1 \ldots Q_k X_k F(\bar{X}_k)$ if and only if $\langle \mathscr{P}_f(\mathbb{N}), \subseteq \rangle \models Q_1 X_1 \subseteq [0, 2^k - 2^{k-1}] Q_2 X_2 \subseteq [0, 2^k - 2^{k-2}] \ldots Q_k X_k \subseteq [0, 2^k - 1] F(\bar{X}_k)$.*

Proof. By Lemmas 3.4 and 3.5, the hypotheses of Theorem 2.1 are satisfied, with $\| A \| = \max(A)$, $H(n, k, m) = m + 2^n$, and $\mu = 0$. We set $m_0 = 0$ and $m_i = H(k-i, i-1, m_{i-1}) = m_{i-1} + 2^{k-i}$. Then $m_i = 2^k - 2^{k-i}$, and by Theorem 2.1

$$\langle \mathscr{P}_f(\mathbb{N}), \subseteq \rangle \models Q_1 X_1 \ldots Q_k X_k F(\bar{X}_k)$$

if and only if

$$\langle \mathscr{P}_f(\mathbb{N}), \subseteq \rangle \models Q_1 X_1 \preceq m_1 \ldots Q_k X_k \preceq m_k F(\bar{X}_k),$$

where

$$X_i \preceq m_i \Leftrightarrow \max(X_i) \leqslant m_i \Leftrightarrow X_i \subseteq [0, m_i]. \quad \square$$

Theorem 3.7. $\operatorname{Th}(\mathscr{P}_f(\mathbb{N}), \subseteq) \in \bigcup_{c>0} \operatorname{ATIME-ALT}(2^{cn}, n)$.

Proof. In a computation, a finite subset X of $\mathbb{N}$, $X \subseteq [0,m]$, can be written as a string $x_0 x_1 \dots x_m \in \{0,1\}^{m+1}$, such that $\forall i\, 0 \leqslant i \leqslant m \Rightarrow (x_i = 1 \Leftrightarrow i \in X)$. Let φ be a sentence with k quantifiers ($k \leqslant |\varphi| = n$). The following procedure decides φ:

(1) Put φ on prenex normal form: $Q_1 X_1 \dots Q_k X_k F(\bar{X}_k)$, which can be done in deterministic polynomial time. The length of $F(\bar{X}_k)$ is $O(n \log n)$, the factor $\log n$ being due to the renaming of variables.

(2) Write a k-tuple $(A_1,\dots,A_k) \in [0, 2^k - 2^{k-1}] \times \cdots \times [0, 2^k - 1]$, where A_i is written in an existential (universal) state if $Q_i = \exists$ ($Q_i = \forall$). This is done in alternating time at most $k2^k \leqslant 2^{2k}$, with at most k alternations.

(3) Verify deterministically that $F(\bar{A}_k)$ is true. This can be done in time $O(2^k n \log n) + p(n \log n)$ for a polynomial p. Indeed, the length of $F(\bar{X}_k)$ is $O(n \log n)$, and the computation of the truth value of an atomic formula $A_i \subseteq A_j$ only needs to read the strings coding A_i and A_j (they can be read simultaneously by putting them on different tapes); this can be done in time at most 2^k. At last, the truth value of the propositional formula with no variable that we obtain is computed in deterministic time $p(n \log n)$ for a polynomial p.

The total time needed by this procedure is at most 2^{cn} for a constant c, with at most k alternations. □

A closer inspection of the proof of Theorem 3.7 leads to the following definitions and theorem.

Definition 3.8. Let $q(\varphi)$ be the number of quantifiers in a sentence φ. Let $a(\varphi)$ be the number of alternations of quantifiers in a prenex normal form of φ which has the smallest such number.

A theory T is in the class of theories BAT (for bounded alternating time) if there are a polynomial p, a constant c and an ATM M which accepts the sentences φ in T in alternating time $2^{cq(\varphi)} p(|\varphi|)$ with at most $a(\varphi)$ alternations.

Theorem 3.9. $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), \subseteq) \in BAT$.

We give a lower bound on the complexity of $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), \subseteq)$ that almost matches the upper bound given by Theorem 3.7.

Proposition 3.10. (i) $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), \subseteq)$ *is* $\bigcup_{c>0} \mathrm{ATIME\text{-}ALT}(2^{cn/\log n}, cn)$*-hard for* $\leqslant_{\mathrm{m}}^{\mathrm{rll}}$.

(ii) $\exists c > 0\ \mathrm{Th}(\mathscr{P}_f(\mathbb{N}), \subseteq) \notin \mathrm{ATIME\text{-}ALT}(2^{cn/\log n}, cn)$.

Proof. Compton and Henson [8, pp. 58–59] prove the following results: any extension, with an infinite model, of the first-order theory of Boolean algebras has a hereditary lower bound of $\mathrm{ATIME\text{-}ALT}(2^{cn/\log n}, cn)$ and is $\bigcup_{c>0} \mathrm{ATIME\text{-}ALT}(2^{cn/\log n}, cn)$-hard for $\leqslant_{\mathrm{m}}^{\mathrm{rll}}$. It is easy to see that their proof yields the same results for $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), \subseteq)$. □

Corollary 3.11. $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), \subseteq)$ *is* $\bigcup_{k>0} \mathrm{AT_1ME\text{-}ALT}(2^{n^k}, n)$*-complete for* $\leqslant_{\mathrm{m}}^{\mathrm{p}}$.

This corollary was stated by Volger [26].

We have focused on the structure $\langle \mathscr{P}_f(\mathbb{N}), \subseteq \rangle$. Now we allow more relations and functions, and we prove that the complexity does not change.

Proposition 3.12. $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), =, \subseteq, \perp,) \in BAT$ *(and, consequently,* $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), \perp) \in BAT$*).*

Proof. Recall that we write $A \perp B$ if A and B are disjoint subsets of $\mathbb{N}$: $A \cap B = \emptyset$.

An inspection of the proof of Theorem 3.7 shows that the fact that the vocabulary equals $\{\subseteq\}$ is used only twice: in Lemma 3.5 and in the computation of the truth value of an atomic formula $A_i \subseteq A_j$. In both cases, the proof is unchanged if the vocabulary is $\{=, \subseteq, \perp\}$. □

The following definition and proposition will allow one to obtain an upper bound on the complexity of a theory T by reducing it to a theory which is known to be in BAT. They will be used in Proposition 3.15 and in the next section.

Definition 3.13. A theory T is $\leqslant_{\mathrm{m}}^{\mathrm{a}}$-reducible to a theory T' if there is a function f computable in deterministic polynomial time, a polynomial r and a constant d, such that for any sentence φ,

(i) $\varphi \in T \Leftrightarrow f(\varphi) \in T'$,
(ii) $f(\varphi)$ is in prenex normal form,
(iii) $|f(\varphi)| \leqslant r(|\varphi|)$,
(iv) $q(f(\varphi)) \leqslant d|\varphi|$,
(v) $a(f(\varphi)) \leqslant |\varphi|$.

Warning: the reduction $\leqslant_{\mathrm{m}}^{\mathrm{a}}$ is not transitive.

Proposition 3.14. *Let* T *and* T' *be two theories. If* $T \leqslant_{\mathrm{m}}^{\mathrm{a}} T'$ *and* $T' \in BAT$*, then* $T \in \bigcup_{c>0} \mathrm{ATIME\text{-}ALT}(2^{cn}, n)$.

Proof. Since $T \leqslant_{\mathrm{m}}^{\mathrm{a}} T'$, there is a function f satisfying the conditions of Definition 3.13. Since $T' \in BAT$, there is a (increasing) polynomial p, a constant c and an ATM M which accepts a sentence ψ in T' in alternating time $2^{cq(\psi)}p(|\psi|)$ with at most $a(\psi)$ alternations.

Let M' be the ATM which on a sentence φ on the vocabulary of T computes $f(\varphi)$ and simulates M on $f(\varphi)$. Then M' accepts sentences in T in alternating time $2^{cq(|f(\varphi)|)}p(|f(\varphi)|) \leqslant 2^{cd|\varphi|}p \circ r(|\varphi|)$ with a number of alternations at most $a(f(\varphi)) \leqslant |\varphi|$. Thus, $T \in \bigcup_{c>0} \mathrm{ATIME\text{-}ALT}(2^{cn}, n)$. □

In the sequel, the class BAT and the reduction $\leqslant_{\mathrm{m}}^{\mathrm{a}}$ are tools used to prove theories to be in $\bigcup_{c>0} \mathrm{ATIME\text{-}ALT}(2^{cn}, n)$, with n alternations. Note that the arguments

would be slightly easier if we had contented ourselves with proving theories to be in $\bigcup_{c>0}$ ATIME-ALT$(2^{cn}, cn)$, with linear number of alternations.

Proposition 3.15. $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), =, \subseteq, \cap, \cup, \perp, \emptyset) \in \bigcup_{c>0}$ ATIME-ALT$(2^{cn}, n)$.

Proof. We prove that $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), =, \subseteq, \cap, \cup, \perp, \emptyset) \leqslant_{\mathrm{m}}^{\mathrm{a}} \mathrm{Th}(\mathscr{P}_f(\mathbb{N}), =, \subseteq, \perp,)$. Then the proposition follows from Propositions 3.12 and 3.14.

Let φ be a sentence on the vocabulary $\{=, \subseteq, \cap, \cup, \perp, \emptyset\}$. We eliminate one by one the symbols $\cap$, $\cup$ and $\emptyset$ from φ according to the following equivalences, where T_1, T_2, T_3 denote terms:

$$T_1 = T_2 \cap T_3 \Leftrightarrow \forall X (X \subseteq T_1) \Leftrightarrow (X \subseteq T_2 \wedge X \subseteq T_3),$$

$$T_1 = T_2 \cup T_3 \Leftrightarrow \forall X (T_1 \subseteq X) \Leftrightarrow (T_2 \subseteq X \wedge T_3 \subseteq X),$$

$$T_1 = \emptyset \Leftrightarrow \forall X (T_1 \subseteq X),$$

$$T_1 \cap T_2 \subseteq T_3 \Leftrightarrow \forall X (X \subseteq T_1 \wedge X \subseteq T_2) \Rightarrow (X \subseteq T_3),$$

$$T_1 \subseteq T_2 \cap T_3 \Leftrightarrow \forall X (X \subseteq T_1) \Rightarrow (X \subseteq T_2 \wedge X \subseteq T_3),$$

$$T_1 \cup T_2 \subseteq T_3 \Leftrightarrow \forall X (T_3 \subseteq X) \Rightarrow (T_1 \subseteq X \wedge T_2 \subseteq X),$$

$$T_1 \subseteq T_2 \cup T_3 \Leftrightarrow \forall X (T_2 \subseteq X \wedge T_3 \subseteq X) \Rightarrow (T_1 \subseteq X),$$

$$\emptyset \subseteq T_1 \Leftrightarrow \forall X (X \subseteq X),$$

$$T_1 \subseteq \emptyset \Leftrightarrow \forall X (T_1 \subseteq X),$$

$$T_1 \perp T_2 \cap T_3 \Leftrightarrow \forall X (X \subseteq T_2 \wedge X \subseteq T_3) \Rightarrow (X \perp T_1),$$

$$T_1 \perp T_2 \cup T_3 \Leftrightarrow \forall X (X \subseteq T_1) \Rightarrow (X \perp T_2 \wedge X \perp T_3),$$

$$T_1 \perp \emptyset \Leftrightarrow \forall X (X \subseteq X).$$

This elimination can be done in deterministic polynomial time. Each elimination of symbol increases the length of the sentence by an additive constant. Thus, the length of the final sentence is linear in the length n of φ and becomes $O(n \log n)$ when the sentence is put in prenex normal form.

Each elimination of symbol introduces only one quantifier. Thus, the number of quantifiers in the final sentence is smaller than the length of φ. Therefore,

$$\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), =, \subseteq, \cap, \cup, \perp, \emptyset) \leqslant_{\mathrm{m}}^{\mathrm{a}} \mathrm{Th}(\mathscr{P}_f(\mathbb{N}), =, \subseteq, \perp,). \qquad \square$$

Of course, the same upper bound holds for theories which are obtained by dropping some symbols, such as $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), =, \cap)$, and $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), =, \cup)$.

We now consider lower bounds on these theories.

Proposition 3.16. *The lower bound of Proposition* 3.10 *holds for* $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), \perp)$, $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), =, \cap)$, *and* $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), =, \cup)$.

Proof. The following equivalences, where X, Y are variables, show that $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), \subseteq)$ can be reduced by $\leqslant_m^{\mathrm{rll}}$ to the theories above.

$$X \subseteq Y \Leftrightarrow \forall Z (Z \perp Y \Rightarrow Z \perp X),$$

$$\Leftrightarrow X \cap Y = X,$$

$$\Leftrightarrow X \cup Y = Y. \quad \square$$

The following theorem will provide us a nice corollary in the next section.

Theorem 3.17. (i) $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}) \cup \{\mathbb{N}\}, =, \subseteq, \perp) \in BAT$.
(ii) $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}) \cup \{\mathbb{N}\}, =, \subseteq, \cap, \cup, \perp, \emptyset) \in \bigcup_{c>0} \mathrm{ATIME\text{-}ALT}(2^{cn}, n)$.

Proof. We prove that $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}) \cup \{\mathbb{N}\}, \subseteq) \in BAT$. Then the first part of the theorem can be derived as in Proposition 3.12 and the second part as in Proposition 3.15.

The set $\mathbb{N}$ cannot be defined in $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), \subseteq)$; thus, we must take again the proofs of Lemmas 3.4–3.6. We limit ourselves to indicate the slight modifications that have to be done to these proofs. We define $\mathscr{P}_f(\mathbb{N})^+ = \mathscr{P}_f(\mathbb{N}) \cup \{\mathbb{N}\}$. We define the family $(E_k^n)^+$ of equivalence relations on $(\mathscr{P}_f(\mathbb{N})^+)^k$ by: if $\bar{A}_k, \bar{B}_k \in (\mathscr{P}_f(\mathbb{N})^+)^k$, then $\bar{A}_k (E_k^n)^+ \bar{B}_k$ if

(i) $\forall i \; 1 \leqslant i \leqslant k \Rightarrow (A_i = \mathbb{N} \Leftrightarrow B_i = \mathbb{N})$,

(ii) $\forall \bar{\varepsilon}_k \in \{-1, 1\}^k \; \mathrm{card}(\bar{\varepsilon}_k \bar{A}_k) \underset{n}{\simeq} \mathrm{card}(\bar{\varepsilon}_k \bar{B}_k)$, where both sides can be infinite. We define $\|\cdot\|^+$ by $\|A\|^+ = \max(A)$ if $A \in \mathscr{P}_f(\mathbb{N}) - \{\emptyset\}$, and $\|\emptyset\|^+ = \|\mathbb{N}\|^+ = 0$. We remark that if an $A_i (1 \leqslant i \leqslant k)$ is equal to $\mathbb{N}$, then either $\bar{\varepsilon}_k \bar{A}_k$ is unchanged (if $\varepsilon_i = 1$), or is empty (if $\varepsilon_i = -1$). This remark makes easy the modifications of the proofs. Lemma 3.4 is stated with $\mathscr{P}_f(\mathbb{N})^+$, $(E_k^n)^+$ and $\|\cdot\|^+$ instead of $\mathscr{P}_f(\mathbb{N})$, E_k^n and $\|\cdot\|$. If $\bar{A}_k, \bar{B}_k \in (\mathscr{P}_f(\mathbb{N})^+)^k$ and $\bar{A}_k (E_k^{n+1})^+ \bar{B}_k$, and if $A_{k+1} \in \mathscr{P}_f(\mathbb{N})^+$, then: if $A_{k+1} = \mathbb{N}$, we choose $B_{k+1} = \mathbb{N}$, else we take B_{k+1} as in the proof of Lemma 3.4. Lemma 3.5 is stated and proved analogously. In the statement of Lemma 3.6, we replace $\mathscr{P}_f(\mathbb{N})$ by $\mathscr{P}_f(\mathbb{N})^+$, and $Q_i X_i \subseteq [0, 2^k - 2^{k-i}]$ by $Q_i X_i \in \mathscr{P}([0, 2^k - 2^{k-i}]) \cup \{\mathbb{N}\}$. In the proof of Theorem 3.7, we code the subset A_i which are equal to $\mathbb{N}$ by a special symbol. The computation of the truth value of an inclusion involving $\mathbb{N}$ is trivial. $\square$

Remark 3.18. The same lower bounds as in Propositions 3.10 and 3.16 hold for $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}) \cup \{\mathbb{N}\}, \subseteq)$ and $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}) \cup \{\mathbb{N}\}, \perp)$.

4. Complexity of theories involving the coprimality relation

For natural numbers a and b, we write $a \perp b$ if a is coprime to b, i.e. if the greatest common divisor of a and b is 1. The use of the same symbol for coprime numbers and disjoint subsets of $\mathbb{N}$ is justified by the following proposition.

Proposition 4.1. (i) $\mathrm{Th}(\mathbb{N}-\{0\}, \perp)=\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), \perp)$,
(ii) $\mathrm{Th}(\mathbb{N}, \perp)=\mathrm{Th}(\mathscr{P}_f(\mathbb{N})\cup\{\mathbb{N}\}, \perp)$.

Proof. Let SF be the set of square-free natural numbers, i.e. the set of numbers which are not divisible by the square of a prime number.

We first prove that $\langle SF, \perp\rangle$ is an elementary substructure of $\langle \mathbb{N}-\{0\}, \perp\rangle$, which implies that $\mathrm{Th}(SF, \perp)=\mathrm{Th}(\mathbb{N}-\{0\}, \perp)$. To show this, it is sufficient (see e.g. [7, p. 108] to show that for any formula $\psi(x, y_1, \ldots, y_n)$, any $a\in\mathbb{N}-\{0\}$, and $b_1, \ldots, b_n\in SF$, such that $\langle \mathbb{N}-\{0\}, \perp\rangle \models \psi(a, b_1, \ldots, b_n)$, there is some $b\in SF$ such that $\langle \mathbb{N}-\{0\}, \perp\rangle \models \psi(b, b_1, \ldots, b_n)$. We choose $b=\prod\{p: p \text{ prime}, p|a\}$. Then $b\in SF$, and any atomic subformula of ψ where x occurs has the same truth value in $\langle \mathbb{N}-\{0\}, \perp\rangle$, whether a or b is substituted for x.

Now $\langle SF, \perp\rangle$ is isomorphic to $\langle \mathscr{P}_f(\mathbb{N}), \perp\rangle$. For any $n\in SF$, let $f(n)$ be the finite subset of $\mathbb{N}$ of numbers i such that the $(i+1)$st prime number p_{i+1} divides n, i.e. $f(n)=\{i\in\mathbb{N}: p_{i+1}|n\}$. Then for any $n, m\in SF$, $n \perp m \Leftrightarrow f(n)\cap f(m)=\emptyset$; thus, $f: SF\to\mathscr{P}_f(\mathbb{N})$ is an isomorphism. Therefore,

$$\mathrm{Th}(\mathbb{N}-\{0\}, \perp)=\mathrm{Th}(SF, \perp)=\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), \perp).$$

The same proof shows that

$$\mathrm{Th}(\mathbb{N}, \perp)=\mathrm{Th}(SF\cup\{0\}, \perp)=\mathrm{Th}(\mathscr{P}_f(\mathbb{N})\cup\{\mathbb{N}\}, \perp). \qquad \square$$

Theorem 4.2. (i) $\mathrm{Th}(\mathbb{N}-\{0\}, \perp)\in BAT\subseteq\bigcup_{c>0}\mathrm{ATIME\text{-}ALT}(2^{cn}, n)$,
(ii) $\mathrm{Th}(\mathbb{N}, \perp)\in BAT\subseteq\bigcup_{c>0}\mathrm{ATIME\text{-}ALT}(2^{cn}, n)$,
(iii) $\exists c>0\ \mathrm{Th}(\mathbb{N}-\{0\}, \perp)\notin\mathrm{ATIME\text{-}ALT}(2^{cn/\log n}, cn)$,
(iv) $\mathrm{Th}(\mathbb{N}-\{0\}, \perp)$ *is* $\bigcup_{c>0}\mathrm{ATIME\text{-}ALT}(2^{cn/\log n}, cn)$*-hard for* $\leqslant_m^{\mathrm{rll}}$.

Proof. The theorem follows from Proposition 4.1 and the results of Section 3. Of course, the lower bounds (iii) and (iv) also hold for $\mathrm{Th}(\mathbb{N}, \perp)$, because the element 0 and so $\mathbb{N}-\{0\}$ can be defined in $\langle \mathbb{N}, \perp\rangle$. $\square$

It is known that multiplication cannot be defined in $\langle \mathbb{N}, \perp\rangle$ (in fact, this is a corollary of the proof of Proposition 4.1, since SF is not closed under $\times$, but is an elementary substructure of $\langle \mathbb{N}-\{0\}, \perp\rangle$). What happens if we add this new function? It is known that $\mathrm{Th}(\mathbb{N}, =, \times)\in\bigcup_{c>0}\mathrm{ATIME\text{-}ALT}(2^{2^{2^{cn}}}, n)$ [3, 4, 10, 20, 21], which shows the great power of multiplication. It could have been thought that adding the binary function $\times$ to $\mathrm{Th}(\mathbb{N}, \perp)$ would have greatly increased the computational complexity of this theory. The following theorem shows, in fact, that this complexity is unaltered.

Warning: we consider the binary function of multiplication, and not the graph of this function, because equality is definable from this graph.

Theorem 4.3. $\mathrm{Th}(\mathbb{N}, \perp, \times) \in \bigcup_{c>0} \mathrm{ATIME\text{-}ALT}(2^{cn}, n)$, *where* $\times$ *is the binary function of multiplication.*

Proof. We prove that $\mathrm{Th}(\mathbb{N}, \perp, \times) \leqslant_m^a \mathrm{Th}(\mathbb{N}, \perp)$. Then the theorem follows from Proposition 3.14 and Theorem 4.2.

Consider a sentence φ in $\mathrm{Th}(\mathbb{N}, \perp, \times)$. The terms in this sentence have the form $x_1 \times x_2 \times \cdots \times x_l$, and the atomic formulas in this sentence have the form $(x_1 \times x_2 \times \cdots \times x_l) \perp (y_1 \times y_2 \times \cdots \times y_m)$. This last formula can be transformed into the equivalent formula $(x_1 \perp y_1) \wedge (x_1 \perp y_2) \wedge \cdots \wedge (x_1 \perp y_m) \wedge (x_2 \perp y_1) \wedge \cdots \wedge (x_l \perp y_m)$ in deterministic polynomial time. Then the sentence φ is transformed in a polynomially longer sentence ψ, but with the same number of quantifiers as φ, such that $\varphi \in \mathrm{Th}(\mathbb{N}, \perp, \times) \Leftrightarrow \psi \in \mathrm{Th}(\mathbb{N}, \perp)$. Thus, $\mathrm{Th}(\mathbb{N}, \perp, \times) \leqslant_m^a \mathrm{Th}(\mathbb{N}, \perp)$. □

Consider $\mathrm{Th}(\mathbb{N} - \{0\}, =, \perp)$. It is known that equality cannot be defined in $\langle \mathbb{N} - \{0\}, \perp \rangle$. On the other hand, it is known that equality and coprimality can be defined in $\langle \mathbb{N} - \{0\}, | \rangle$, and that $\mathrm{Th}(\mathbb{N} - \{0\}, |) \in \bigcup_{c>0} \mathrm{ATIME\text{-}ALT}(2^{cn^2 \log n}, n)$ [26]. Therefore, the following theorem is an improvement on the result given by the reduction of $\mathrm{Th}(\mathbb{N} - \{0\}, =, \perp)$ to the theory of divisibility.

Theorem 4.4. $\mathrm{Th}(\mathbb{N} - \{0\}, =, \perp) \in \bigcup_{c>0} \mathrm{ATIME\text{-}ALT}(2^{cn^2}, n)$.

Proof. We have not been able to simply reduce the complexity of $\mathrm{Th}(\mathbb{N} - \{0\}, =, \perp)$ to that one of $\mathrm{Th}(\mathbb{N} - \{0\}, \perp)$. We come back to the basic method. For any $a \in \mathbb{N} - \{0\}$, we set $\mathrm{Supp}(a) = \{p : p \text{ prime}, p | a\}$ and we denote by $\overline{\mathrm{Supp}(a_k)}$ the k-tuple $(\mathrm{Supp}(a_1), \ldots, \mathrm{Supp}(a_k))$. We define a family E_k^n of equivalence relations on $(\mathbb{N} - \{0\})^k$: for any $\bar{a}_k, \bar{b}_k, \bar{a}_k E_k^n \bar{b}_k$ if

(i) $\forall i, j \leqslant k \; a_i = a_j \Leftrightarrow b_i = b_j$,

(ii) $\forall \bar{\varepsilon}_k \in \{-1, 1\}^k \; \mathrm{card}(\bar{\varepsilon}_k \overline{\mathrm{Supp}(a_k)}) \underset{n}{\simeq} \mathrm{card}(\bar{\varepsilon}_k \overline{\mathrm{Supp}(b_k)})$.

As in Theorem 3.7, the proof consists in three lemmas.

Lemma 4.5. *Let* $\bar{a}_k, \bar{b}_k \in (\mathbb{N} - \{0\})^k$ *such that* $\bar{a}_k E_k^{n+1} \bar{b}_k$. *Then for any* $a_{k+1} \in \mathbb{N} - \{0\}$, *there is a* $b_{k+1} \in \mathbb{N} - \{0\}$ *such that* $\bar{a}_{k+1} E_{k+1}^n \bar{b}_{k+1}$. *If, moreover,* $\forall i \; 1 \leqslant i \leqslant k \Rightarrow b_i \leqslant m$ *and* $m \geqslant 1$, *then we can choose* b_{k+1} *such that* $b_{k+1} \leqslant m^{(k+1)(k+2^n)}((n+1)2^{n+1})^{(k+1)2^n}$.

Proof of Lemma 4.5. Suppose that $\bar{a}_k E_k^{n+1} \bar{b}_k$ and let $a_{k+1} \in \mathbb{N} - \{0\}$. If $a_{k+1} = a_i$ for any $i, 1 \leqslant i \leqslant k$, then we take $b_{k+1} = b_i$. Else, the proof is similar to the one of Lemma 3.4, where the A_i's are replaced by the $\mathrm{Supp}(a_i)$'s. We first construct b by the following procedure:

- if $\mathrm{card}(\mathrm{Supp}(a_{k+1}) \cap \bar{\varepsilon}_k \overline{\mathrm{Supp}(a_k)}) < \mathrm{card}(-\mathrm{Supp}(a_{k+1}) \cap \bar{\varepsilon}_k \overline{\mathrm{Supp}(a_k)})$, then we put in $\mathrm{Supp}(b) \cap \bar{\varepsilon}_k \overline{\mathrm{Supp}(b_k)}$ the $\min(2^n, \mathrm{card}(\mathrm{Supp}(a_{k+1}) \cap \bar{\varepsilon}_k \overline{\mathrm{Supp}(a_k)}))$ smallest members of $\bar{\varepsilon}_k \overline{\mathrm{Supp}(b_k)}$.

– else, we put in $\mathrm{Supp}(b)\cap\bar{\varepsilon}_k\overline{\mathrm{Supp}(b_k)}$ the $\mathrm{card}(\bar{\varepsilon}_k\overline{\mathrm{Supp}(b_k)})-\min(2^n, \mathrm{card}(-\mathrm{Supp}(a_{k+1})\cap\bar{\varepsilon}_k\overline{\mathrm{Supp}(a_k)}))$ smallest members of $\bar{\varepsilon}_k\overline{\mathrm{Supp}(b_k)}$.

Note that the number b so constructed is square-free, and it is not sure that b suits. We must have, for any i, $1\leqslant i\leqslant k, b_{k+1}\neq b_i$. So we choose among the numbers $b^j: 1\leqslant j\leqslant k+1$, the least one that suits, i.e.

$$b_{k+1}=\min\{b^j:\ 1\leqslant j\leqslant k+1 \text{ and } \forall i\ 1\leqslant i\leqslant k\Rightarrow b^j\neq b_i\}.$$

Then the same analysis as in Lemma 3.4 gives $\bar{a}_{k+1}\,E^n_{k+1}\,\bar{b}_{k+1}$.

Suppose that $\forall i\ \ 1\leqslant i\leqslant k\Rightarrow b_i\leqslant m$, where $m\geqslant 1$. Then either $b_{k+1}=b_i\leqslant m$ or $b_{k+1}\leqslant b^{k+1}$, where $b\in SF$. In this second case, the prime factors of b which are inside $\bigcup_{i=1}^k \mathrm{Supp}(b_i)$ have a product at most $\prod_{i=1}^k b_i\leqslant m^k$. And the prime factors of b which are outside $\bigcup_{i=1}^k \mathrm{Supp}(b_i)$ are those from $\mathrm{Supp}(b)\cap\bar{\varepsilon}_k^{\infty}\overline{\mathrm{Supp}(b_k)}$. Their number is at most 2^n, and they are the smallest ones. Thus, if p_u is the greatest prime number less than m, they are at most the prime numbers $p_{u+1}, p_{u+2},\ldots, p_{u+2^n}$. As b_{k+1} is square-free, we obtain

$$b\leqslant m^k\prod_{j=1}^{2^n} p_{u+j}\leqslant m^k(p_{u+2^n})^{2^n}.$$

It is known that

(i) $\forall s,t\geqslant 1\ \ p_{s+t}<p_sp_t$,

(ii) $\forall n\geqslant 1\ \ p_n\leqslant 2n\log(2n)$

(see e.g. [22, p. 190]). Hence,

$$p_{u+2^n}\leqslant p_up_{2^n}\leqslant m\,2^{n+1}(n+1), \quad \text{and} \quad b\leqslant m^{k+2^n}((n+1)2^{n+1})^{2^n}.$$

Therefore,

$$b_{k+1}\leqslant b^{k+1}\leqslant m^{(k+1)(k+2^n)}((n+1)2^{n+1})^{(k+1)2^n}. \qquad \square$$

Lemma 4.6. *If $\bar{a}_k\,E^0_k\,\bar{b}_k$, then $\bar{a}_k$ and $\bar{b}_k$ satisfy the same atomic formulas.*

Proof of Lemma 4.6. $\bar{a}_k\,E^0_k\,\bar{b}_k$ if and only if $\forall i,j\leqslant k\ a_i=a_j\Leftrightarrow b_i=b_j$, and $\forall\bar{\varepsilon}_k\in\{-1,1\}^k$ either $\bar{\varepsilon}_k\overline{\mathrm{Supp}(a_k)}=\bar{\varepsilon}_k\overline{\mathrm{Supp}(b_k)}=\emptyset$, or both $\bar{\varepsilon}_k\overline{\mathrm{Supp}(a_k)}$ and $\bar{\varepsilon}_k\overline{\mathrm{Supp}(b_k)}$ are nonempty. This implies that

$$\forall i,j\quad 1\leqslant i,j\leqslant k\Rightarrow(a_i\perp a_j\Leftrightarrow b_i\perp b_j),$$

because

$$a_i\perp a_j \Leftrightarrow \mathrm{Supp}(a_i)\cap\mathrm{Supp}(a_j)=\emptyset$$

$$\Leftrightarrow \forall\bar{\varepsilon}_k\in\{-1,1\}^k(\varepsilon_i=\varepsilon_j=1\Rightarrow\bar{\varepsilon}_k\overline{\mathrm{Supp}(a_k)}=\emptyset). \qquad \square$$

Lemma 4.7. *Let $Q_1x_1\ldots Q_kx_kF(\bar{x}_k)$ be a sentence, with $F(\bar{x}_k)$ quantifier-free. Then*

$$\langle\mathbb{N}-\{0\},=,\perp\rangle\models Q_1x_1\ldots Q_kx_kF(\bar{x}_k)$$

if and only if

$$\langle \mathbb{N}-\{0\}, =, \perp \rangle \models Q_1 x_1 \leqslant m_1 \ldots Q_k x_k \leqslant m_k F(\bar{x}_k),$$

where $m_i = 2^{2^{2i\log(i+1)+i(2k-i)}}$.

Proof of Lemma 4.7. We apply Theorem 2.1, with the identity as a norm, $\mu = 1$ and

$$H(n,k,m) = m^{(k+1)(k+2^n)}((n+1)2^{n+1})^{(k+1)2^n}.$$

We search for $1 \leqslant m_0 \leqslant m_1 \leqslant \cdots \leqslant m_k$ such that

$$\forall i \quad 1 \leqslant i \leqslant k \Rightarrow m_i \geqslant H(k-i, i-1, m_{i-1}).$$

Let $l_i = \log m_i$. Then this condition becomes

$$l_i \geqslant i(i-1+2^{k-i})l_{i-1} + i2^{k-i}[(k-i+1)+\log(k-i+1)],$$

and it can be (tediously) verified that $l_i = 2^{2i\log(i+1)+i(2k-i)}$ suits. □

Proof of Theorem 4.4 (*conclusion*). Given a sentence φ of length n, with k quantifiers, we put it in prenex normal form $Q_1 x_1 \ldots Q_k x_k F(\bar{x}_k)$. Then we write $(a_1, \ldots, a_k) \in [0, m_1] \times \cdots \times [0, m_k]$, where a_i is written in an existential (universal) state if $Q_i = \exists$ ($Q_i = \forall$). This can be done in alternating time at most $k \log m_k \leqslant 2^{4k^2}$, and at most k alternations. Then $F(\bar{a}_k)$ is deterministically verified, which can be done in time $(|F(\bar{x}_k)| + |\bar{a}_k|)^d \leqslant n^d 2^{4dk^2}$ for a fixed constant d.

As $k \leqslant n$, the total time is $2^{O(n^2)}$ and there are at most n alternations. □

Remark 4.8. We have seen in the proof of Proposition 4.1 that $\mathrm{Th}(\mathbb{N}-\{0\}, \perp) = \mathrm{Th}(SF, \perp)$. However, $\mathrm{Th}(\mathbb{N}-\{0\}, =, \perp) \neq \mathrm{Th}(SF, =, \perp)$. Indeed, let φ be the sentence $\exists x\, \exists y\, (\neg(x=y) \wedge \forall z\, (z \perp x \Leftrightarrow z \perp y))$. Then $\langle \mathbb{N}-\{0\}, =, \perp \rangle \models \varphi$, but $\langle SF, =, \perp \rangle \not\models \varphi$.

5. Complexity of theories involving functions

Up to now, we have limited ourselves to the study of the relations and functions $=, \leqslant, |, \perp, S, +, \times$ on $\mathbb{N}$. Of course, many other relations and functions can be defined on $\mathbb{N}$. The most relevant ones are the functions $2x, x^2$ and 2^x. These functions can be added to the structures we have considered, and it can be asked what the complexities of the theories of the structures so constituted are. In this section, we only graze the subject. The proofs of the results we give mainly use methods we saw in the previous sections.

On the side of theories with great complexities, it is known that $\mathrm{Th}(\mathbb{N}, =, +, 2^x)$ is decidable [24], but not elementary recursive [8, p. 55]. $\mathrm{Th}(\mathbb{N}, \leqslant, x^2)$ is decidable [24], but its complexity is not known.

On the other side, we have the following theorem.

Theorem 5.1. $\mathrm{Th}(\mathbb{N}, =, 2x)$, $\mathrm{Th}(\mathbb{N}, =, x^2)$ *and* $\mathrm{Th}(\mathbb{N}, =, 2^x)$ *are* PSPACE-*complete.*

Proof. We first prove that the structures we consider are isomorphic to a simple structure. Let B be a finite set disjoint from $\mathbb{N} \times \mathbb{N}$, and let $A = B \cup (\mathbb{N} \times \mathbb{N})$. Let $S: A \to A$ be defined by

$$S(b) = b \qquad \text{if } b \in B,$$
$$S((x, y)) = (x + 1, y) \qquad \text{if } (x, y) \in \mathbb{N} \times \mathbb{N}.$$

Then

$$\langle \mathbb{N}, =, 2x \rangle \cong \langle A_1, =, S \rangle \qquad \text{for } B = B_1 = \{b_1\},$$
$$\langle \mathbb{N}, =, x^2 \rangle \cong \langle A_2, =, S \rangle \qquad \text{for } B = B_2 = \{b_1, b_2\},$$
$$\langle \mathbb{N}, =, 2^x \rangle \cong \langle A_3, =, S \rangle \qquad \text{for } B = B_3 = \emptyset.$$

Let $f_1(x) = 2x$, $f_2(x) = x^2$, $f_3(x) = 2^x$. We describe the isomorphisms

$$g_i: \langle A_i, =, S \rangle \to \langle \mathbb{N}, =, f_i \rangle \quad \text{for } i = 1, 2, 3.$$

For the function $f_1(x) = 2x$, the isomorphism g_1 is given by $g_1(b_1) = 0$, $g_1((n, p)) = 2^n(2p + 1)$ if $n, p \in \mathbb{N}$.

For the function $f_2(x) = x^2$, the isomorphism g_2 is given by $g_2(b_1) = 0$, $g_2(b_2) = 1$, $g_2((n, p)) = u_p^{2^n}$ if $n, p \in \mathbb{N}$, where u_p is the $(p+1)$st number which is not a square ($u_0 = 2$, $u_1 = 3$, $u_2 = 5, \ldots$).

For the function $f_3(x) = 2^x$, the isomorphism g_3 is defined by induction by $g_3((0, p)) = w_p$ if $p \in \mathbb{N}$, and $g_3((n+1, p)) = 2^{g_3((n, p))}$ if $n \in \mathbb{N}$, $p \in \mathbb{N}$, where w_p is the $(p+1)$st number which is not a power of 2 ($w_0 = 0$, $w_1 = 3$, $w_2 = 5, \ldots$).

It can be easily seen that, for $i = 1, 2, 3$, g_i is one-to-one and onto, and $f_i \circ g_i = g_i \circ S$.

We are brought to the analysis of the complexity of $\mathrm{Th}(B \cup (\mathbb{N} \times \mathbb{N}), =, S)$. This theory is PSPACE-hard since it contains the theory of equality on a domain with more than one element. We do not detail the proof that this theory is in PSPACE, for it is only a very special case of the proof in [10] that gives the complexity of the theory of a one-to-one unary function. We only state the two basic lemmas.

We define a (possibly negative) distance on A. For any $a_1, a_2 \in A$,

$$d(a_1, a_2) = \begin{cases} x_2 - x_1 & \text{if } a_1 = (x_1, y),\ a_2 = (x_2, y) \in \mathbb{N} \times \mathbb{N}, \\ \infty & \text{otherwise.} \end{cases}$$

For any $n \in \mathbb{N}$, we define the following equivalence relation on $A \times A$. For any $(a_1, a_2), (b_1, b_2) \in A \times A$, $(a_1, a_2) \underset{n}{\equiv} (b_1, b_2)$ if $\forall q \in \mathbb{Z}$

$$|q| \leqslant 2^n \Rightarrow (d(a_1, a_2) = q \Leftrightarrow d(b_1, b_2) = q).$$

For any $n, k \in \mathbb{N}$, $k \geqslant 1$, we define the equivalence relation E_k^n on A by: for any $\bar{a}_k, \bar{b}_k \in A^k$, $\bar{a}_k E_k^n \bar{b}_k$ if

(i) $\forall c \in B \ \forall i \ 1 \leqslant i \leqslant k \Rightarrow (a_i = c \Leftrightarrow b_i = c)$,

(ii) $\forall i, j \ 1 \leqslant i, j \leqslant k \Rightarrow (a_i, a_j) \underset{n}{\equiv} (b_i, b_j)$,

(iii) $\forall i \ 1 \leqslant i \leqslant k \Rightarrow d(0_{a_i}, a_i) \underset{n}{\simeq} d(0_{b_i}, b_i)$,

where $0_c = c$ if $c \in B$, and $0_{(x,y)} = (0, y)$.

We define a norm on A by $\| c \| = (0,0)$ if $c \in B$, and $\| (x, y) \| = (x, y)$. We define an order $\leqslant$ on $\mathbb{N} \times \mathbb{N}$ by $(x_1, y_1) \leqslant (x_2, y_2)$ if $x_1 \leqslant x_2$ and $y_1 \leqslant y_2$. Then we have the following lemmas.

Lemma 5.2. *Let $n, k \in \mathbb{N}$, $k \geqslant 1$, $\bar{a}_k, \bar{b}_k \in A^k$, and $m, m' \in \mathbb{N}$ such that $\bar{a}_k E_k^{n+1} \bar{b}_k$ and $\forall i \ 1 \leqslant i \leqslant k \Rightarrow \| b_i \| \leqslant (m, m')$. For any $a_{k+1} \in A$, there is a $b_{k+1} \in A$ such that $\bar{a}_{k+1} E_{k+1}^n \bar{b}_{k+1}$ and $\| b_{k+1} \| \leqslant (m + 2^n, \max(m', k+1))$.*

Lemma 5.3. *Let $k \in \mathbb{N} - \{0\}$, and $Q_1 x_1 \ldots Q_k x_k F(\bar{x}_k)$ be a sentence with $F(\bar{x}_k)$ quantifier-free. Then*

$$\langle A, =, S \rangle \models Q_1 x_1 \ldots Q_k x_k F(\bar{x}_k)$$

if and only if

$$\langle A, =, S \rangle \models Q_1 x_1 \preceq (m_1, m_1') \ldots Q_k x_k \preceq (m_k, m_k') F(\bar{x}_k),$$

where

$$\forall i \quad 1 \leqslant i \leqslant k \ \Rightarrow \ m_i = 2^k - 2^{k-i} \text{ and } m_i' = i.$$

From Lemma 5.3 it is easily seen that $\mathrm{Th}(A, =, S)$ is in PSPACE. □

Adding a function to a structure can deeply alter the complexity of its theory. For example, in $\langle \mathbb{N}, =, +, x^2 \rangle$ we can define $\times$ by

$$z = xy \Leftrightarrow (x+y)^2 = x^2 + y^2 + z + z.$$

In $\langle \mathbb{N}, =, \times, 2^x \rangle$ we can define $+$ by

$$z = x + y \Leftrightarrow 2^z = 2^x \times 2^y.$$

In $\langle \mathbb{N}, |, 2^x \rangle$, we can define $\leqslant$ by

$$x \leqslant y \Leftrightarrow 2^x | 2^y.$$

So the theories of these structures are undecidable. However, the following theorem shows that adding these functions to $\langle \mathbb{N}, \perp \rangle$ does not change the complexity of its theory.

Theorem 5.4. $\mathrm{Th}(\mathbb{N}, \perp, \times, 2x, x^2, 2^x) \in \bigcup_{c>0} \mathrm{ATIME\text{-}ALT}(2^{cn}, n)$.

Proof. We begin by giving two preliminary remarks.

First, note that, if t_1 is a term from the vocabulary $\{\times, 2x, x^2, 2^x\}$, then it is very easy to express that $t_1 = 0$ using only the nonlogical symbol $\perp$. We prove this by induction on the structure of the term t_1. If $t_1 = 2^{t_2}$, this formula is false. If $t_1 = 2t_2$ or $t_1 = t_2^2$, this formula is equivalent to $t_2 = 0$. If $t_1 = t_2 \times t_3$, this formula is equivalent to $(t_2 = 0) \vee (t_3 = 0)$. At last, if t_1 is a variable, then this formula is equivalent to $\forall y (y \perp t_1 \Rightarrow y \perp y)$. Consequently, from now on in this proof, we freely use the notation $t_1 = 0$ to mean an equivalent formula made according to the rules above.

Second, note that, if a term t_1 is within the scope of a function 2^x, i.e. is a proper subterm of 2^{t_2}, then, for atomic formulas built with the sole relation $\perp$, it only matters whether or not $t_1 = 0$.

We introduce the constant 2, and we prove that $\mathrm{Th}(\mathbb{N}, \perp, \times, 2x, x^2, 2^x) \leqslant_{\mathrm{m}}^{\mathrm{a}} \mathrm{Th}(\mathbb{N}, \perp, 2)$. Let φ be a sentence in $\mathrm{Th}(\mathbb{N}, \perp, \times\, 2x, x^2, 2^x)$. We eliminate the function $2x$ by replacing each occurrence of $2t_1$, where t_1 is a term, by $2 \times t_1$. Then we eliminate the function x^2 by replacing each occurrence of t_1^2, where t_1 is a term, by t_1. This can be justified by noting that either a term is within the scope of a function 2^x, and then, by the second preliminary remark, it does not matter whether it is squared or not, or this term is not within the scope of a function 2^x, and then has the same relation of coprimality with other terms, whether it is squared or not.

When these eliminations of $2x$ and x^2 are done, the atomic formulas contain only the nonlogical symbols $\times, \perp, 2^x$ and 2, and so have the form

$$(t_1 \times \cdots \times t_p \times 2^{t_{p+1}} \times \cdots \times 2^{t_{p+q}}) \perp (u_1 \times \cdots \times u_r \times 2^{u_{r+1}} \times \cdots \times 2^{u_{r+s}}),$$

where $p, q, r, s \in \mathbb{N}, t_1, \ldots, t_p, u_1, \ldots, u_r$ are variables or the constant 2, and $t_{p+1}, \ldots, t_{p+q}, u_{r+1}, \ldots, u_{r+s}$ are terms from the vocabulary $\{2, \times, 2^x\}$.

We denote by $T = 0$ $(U = 0)$ the formula $(t_{p+1} = 0) \wedge \cdots \wedge (t_{p+q} = 0)$ $((u_{r+1} = 0) \wedge \cdots \wedge (u_{r+s} = 0))$. Then such an atomic formula is equivalent to

$$(t_1 \times \cdots \times t_p \perp u_1 \times \cdots \times u_r) \wedge (t_1 \times \cdots \times t_p \perp 2 \vee U = 0) \wedge$$

$$(u_1 \times \cdots \times u_r \perp 2 \vee T = 0) \wedge (T = 0 \vee U = 0).$$

Using the first preliminary remark, the formulas $T = 0$ and $U = 0$ can be replaced by equivalent formulas on the vocabulary $\{\perp\}$. The symbol $\times$ is eliminated exactly as in the proof of Theorem 4.3. So the initial sentence φ is reduced in deterministic polynomial time to a sentence ψ (in prenex normal form) on the vocabulary $\{\perp, 2\}$, such that ψ is polynomially longer than φ, $q(\psi) \leqslant 2|\varphi|$, $a(\psi) \leqslant |\varphi|$ and $\varphi \in \mathrm{Th}(\mathbb{N}, \perp, \times, 2x, x^2, 2^x) \Leftrightarrow \psi \in \mathrm{Th}(\mathbb{N}, \perp, 2)$. Therefore, $\mathrm{Th}(\mathbb{N}, \perp, \times, 2x, x^2, 2^x) \leqslant_{\mathrm{m}}^{\mathrm{a}} \mathrm{Th}(\mathbb{N}, \perp, 2)$.

In the final stage, we prove that $\mathrm{Th}(\mathbb{N}, \perp, 2) \in BAT$. The proof of Proposition 4.1 shows that $\mathrm{Th}(\mathbb{N}, \perp, 2) = \mathrm{Th}(SF \cup \{0\}, \perp, 2)$, and $\langle SF \cup \{0\}, \perp, 2 \rangle$ is isomorphic

to $\langle \mathscr{P}_f(\mathbb{N}) \cup \{\mathbb{N}\}, \perp, \{0\}\rangle$. Thus, we are brought to the analysis of $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}) \cup \{\mathbb{N}\}, \perp, \{0\})$. This analysis parallels that of $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}) \cup \{\mathbb{N}\}, \perp)$ in Theorem 3.17. The main change is to add to the definition of $(E_k^n)^+$ the condition

$$\forall i \quad 1 \leqslant i \leqslant k \Rightarrow (A_i = \{0\} \Leftrightarrow B_i = \{0\}).$$

Thus, $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}) \cup \{\mathbb{N}\}, \perp, \{0\}) \in BAT$.

We have proved that

$$\mathrm{Th}(\mathbb{N}, \perp, \times, 2x, x^2, 2^x) \leqslant_{\mathrm{m}}^{\mathrm{a}} \mathrm{Th}(\mathbb{N}, \perp, 2) = \mathrm{Th}(\mathscr{P}_f(\mathbb{N}) \cup \{\mathbb{N}\}, \perp, \{0\}) \in BAT.$$

Therefore,

$$\mathrm{Th}(\mathbb{N}, \perp, \times, 2x, x^2, 2^x) \in \bigcup_{c>0} \mathrm{ATIME\text{-}ALT}(2^{cn}, n)$$

by Proposition 3.14. □

6. Conclusion

We are now in a position to answer the question of what happens to the complexity of $\mathrm{Th}(\mathbb{N}, =, \leqslant, |, \perp, S, +, \times)$ if we drop some of these relations or functions from the structure. Only five cases are possible:

(i) The theory is undecidable. This holds if and only if both S and $\perp$ are definable in the structure.

(ii) The theory is $\mathrm{Th}(\mathbb{N}, =, |, \perp, \times)$ (i.e. $\mathrm{Th}(\mathbb{N}, =, \times)$), which is in $\bigcup_{c>0} \mathrm{ATIME\text{-}ALT}(2^{2^{cn}}, n)$, and is complete for $\bigcup_{k>0} \mathrm{ATIME\text{-}ALT}(2^{2^{n^k}}, n)$ for $\leqslant_{\mathrm{m}}^{\mathrm{p}}$.

(iii) The theory is $\mathrm{Th}(\mathbb{N}, =, S, \leqslant, +)$ (i.e. $\mathrm{Th}(\mathbb{N}, =, +)$), which is in $\bigcup_{c>0} \mathrm{ATIME\text{-}ALT}(2^{2^{cn}}, n)$ and is complete for $\bigcup_{k>0} \mathrm{ATIME\text{-}ALT}(2^{2^{n^k}}, n)$ for $\leqslant_{\mathrm{m}}^{\mathrm{p}}$.

(iv) The theory is one of the following: $\mathrm{Th}(\mathbb{N}, =, |, \perp)$ (i.e. $\mathrm{Th}(\mathbb{N}, |)$), $\mathrm{Th}(\mathbb{N}, =, \perp)$, $\mathrm{Th}(\mathbb{N}, \perp, \times)$ or $\mathrm{Th}(\mathbb{N}, \perp)$, which are in $\bigcup_{c>0} \mathrm{ATIME\text{-}ALT}(2^{cf(n)}, n)$, respectively, for $f(n) = n^2 \log n$, $f(n) = n^2$, $f(n) = n$ and $f(n) = n$, and are complete for $\bigcup_{k>0} \mathrm{ATIME\text{-}ALT}(2^{n^k}, n)$ for $\leqslant_{\mathrm{m}}^{\mathrm{p}}$.

(v) The theory is one of the following: $\mathrm{Th}(\mathbb{N}, =, S, \leqslant)$ (i.e. $\mathrm{Th}(\mathbb{N}, \leqslant)$), $\mathrm{Th}(\mathbb{N}, =, S)$ or $\mathrm{Th}(\mathbb{N}, =)$, which are in $\bigcup_{c>0} \mathrm{ATIME\text{-}ALT}(cn^2, n)$ and are PSPACE-complete for $\leqslant_{\mathrm{m}}^{\mathrm{p}}$.

Logical results (axiomatization, finite axiomatizability, elimination of quantifiers, etc.) involving $\mathrm{Th}(\mathscr{P}_f(\mathbb{N}), \subseteq)$, $\mathrm{Th}(\mathbb{N}, \perp)$, $\mathrm{Th}(\mathbb{N}, =, \perp)$, $\mathrm{Th}(\mathbb{N}, |)$ and $\mathrm{Th}(\mathbb{N}, =, \times)$ can be found in [5].

As we have seen in Section 5, adding one of the functions $2x, x^2$ or 2^x can either deeply alter or leave unchanged the complexity of the theory of a structure. We have only grazed this subject, and many open problems are left open.

Acknowledgment

Many thanks to Serge Grigorieff for helpful discussions and comments.

References

[1] J.L. Balcázar, J. Díaz and J. Gabarró, *Structural Complexity I* (Springer, Berlin, 1988).
[2] J.L. Balcázar, J. Díaz and J. Gabarró, *Structural Complexity II* (Springer, Berlin, 1990).
[3] L. Berman, Precise bounds for Presburger arithmetic and the reals with addition, in: *Proc. 18th Symp. on Foundations of Computer Science*, IEEE (1977) 95–99.
[4] L. Berman, The complexity of logical theories, *Theoret. Comput. Sci.* **11** (1980) 71–77.
[5] P. Cegielski, Quelques contributions à l'étude des arithmétiques faibles, Thèse d'État, Université Paris 7, and Publ. LITP 90.77, 1990.
[6] A.K. Chandra, D.C. Kozen and L.J. Stockmeyer, Alternation, *J. ACM* **28** (1981) 114–133.
[7] C.C. Chang and H.J. Keisler, *Model Theory* (North-Holland, Amsterdam, 1973).
[8] K.J. Compton and C.W. Henson, A uniform method for proving lower bounds on the computational complexity of logical theories, *Ann. Pure Appl. Logic* **48** (1990) 1–79.
[9] D.C. Cooper, Theorem-proving in arithmetic without multiplication, *Mach. Intell.* **7** (1972) 91–100.
[10] J. Ferrante and C.W. Rackoff, *The Computational Complexity of Logical Theories*, Lecture Notes in Mathematics, Vol. 718 (Springer, Berlin, 1979).
[11] M.J. Fischer and M.O. Rabin, Super-exponential complexity of Presburger arithmetic, in: R.M. Karp, ed., *Complexity of Computation*, SIAM-AMS Proceedings **7** (AMS, Providence, RI, 1974) 27–41.
[12] J.E. Hopcroft and J.D. Ullman, *Introduction to Automata Theory, Languages, and Computation* (Addison-Wesley, Reading, MA, 1979).
[13] D.C. Kozen, Complexity of Boolean algebras, *Theoret. Comput. Sci.* **10** (1980) 221–247.
[14] L. Lo, On the computational complexity of the theory of abelian groups, *Ann. Pure Appl. Logic* **37** (1988) 205–248.
[15] P. Michel, Borne supérieure de la complexité de la théorie de $\mathbb{N}$ muni de la relation de divisibilité, in: C. Berline, K. McAloon and J.-P. Ressayre, eds., *Model Theory and Arithmetic*, Lecture Notes in Mathematics, Vol. 890 (Springer, Berlin, 1981) 242–250.
[16] A. Mostowski, On direct product of theories, *J. Symbolic Logic* **17** (1952) 1–31.
[17] D.C. Oppen, Elementary bounds for Presburger arithmetic, in: *Proc. 5th ACM Symp. on Theory of Computing*, ACM (1973) 34–37.
[18] D.C. Oppen, A $2^{2^{2^{pn}}}$ upper bound on the complexity of Presburger arithmetic, *J. Comput. System Sci.* **16** (1978) 323–332.
[19] M. Presburger, Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt, in: *Comptes Rendus du 1er Congrès des Mathématiciens des Pays Slaves*, Warsaw (1930) 92–101, 395.
[20] C.W. Rackoff, Complexity of some logical theories, Project MAC TR-144, MIT, Cambridge, MA, 1975.
[21] C.W. Rackoff, On the complexity of the theories of weak direct powers, *J. Symbolic Logic* **41** (1976) 561–573.
[22] P. Ribenboim, *The Book of Prime Number Records* (Springer, New York, 1988).
[23] J. Robinson, Definability and decision problem in arithmetic, *J. Symbolic Logic* **14** (1949) 98–114.
[24] A.L. Semenov, Logical theories of one-place functions on the set of natural numbers, *Math. USSR-Izv.* **22** (1984) (Russian original: 1983) 587–618.
[25] T. Skolem, Über einige Satzfunktionen in der Arithmetik, *Skrifter utgitt av Det Norske Videnskaps-Akademi i Oslo, I. Matematisk-naturvidenskapelig klasse*, Oslo (1931).
[26] H. Volger, Turing machines with linear alternation, theories of bounded concatenation and the decision problem of first order theories, *Theoret. Comput. Sci.* **23** (1983) 333–337.
[27] A. Woods, Some problems in logic and number theory and their connections, Thesis, University of Manchester, 1981.